TITLE OF THE INVENTION

Data Recording Method and Apparatus, Data Reproducing Method and Apparatus, and Data Recording and/or Reproducing System

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention relates to a data recording method and apparatus, a data reproducing method and apparatus, and a data recording and/or reproducing system, and particularly to a data recording method and apparatus, a data reproducing method and apparatus, and a data recording and/or reproducing system to prevent illegal copy of data recorded on a disc-shaped recording medium.

Description of Related Art

Occasionally, copying data such as digital contents data recorded on a disc-shaped recording medium etc. to another recording medium is not restricted. On the other hand, such copying is sometimes restricted or completely prohibited so as not to infringe copyright of data. In case copying data is required to be restricted or prohibited, some countermeasures have to be taken. The contents data are, for example, music, image, program, and text data. Identification information (ID) has been used to encrypt contents data or contents keys so as to prevent copying data recorded on the disc-shaped recording medium etc.

In case a data processing unit for processing contents data to be recorded

and a data recording unit for recording data to a recording medium are mounted in the same apparatus, printed board, or chip, and those units are connected by their interfaces which does not output data to outside thereof, copying data can be prevented.

On the other hand, in case the data processing unit and data recording unit are mounted in different apparatuses and those apparatuses are connected by their general interfaces, data transmitted via those interfaces can be taken out from those apparatuses, which enables copying data.

Even though the data processing unit and data recording unit are mounted in the same apparatus or substrate, copying data becomes possible by monitoring data transmitted between those units via a data line connecting them.

## SUMMARY OF THE INVENTION

It is therefore an object of the present invention to overcome the above-mentioned drawbacks by providing a data recording apparatus, a data reproducing apparatus, and a data recording and/or reproducing system, which is configured such that, even though the data transmitted between a data processing unit and data recording unit is monitored, the monitored data can hardly be read, and thus can prevent copy of data and effectively protect data.

It is another object of the present invention to provide a data recording method and a data reproducing method to implement the data recording apparatus

and data reproducing apparatus.

According to the present invention, when recording digital data to a recording medium,

independent write identification information is generated for each recording of the digital data,

data identification information of the digital data and data control information are encrypted by the use of the write identification information, and

at least the encrypted data identification information and data control information, and the write identification information are recorded to the recording medium.

According to the present invention, there is provided a data recording and/or reproducing system which has a data processing apparatus for encrypting data identification information of digital data and data control information, and a data recording and/or reproducing apparatus for recording the encrypted data identification information and data control information from the data processing apparatus to a recording medium,

wherein the data recording and/or reproducing apparatus has means for generating independent write identification information for each recording of the digital data, and means for recording the encrypted data from the data processing apparatus and write identification information to the recording medium, and

wherein the data processing apparatus encrypts the data identification

information of the digital data and data control information by the use of the write identification information from the data recording and/or reproducing apparatus, and transmits the encrypted data to the data recording and/or reproducing apparatus.

The digital data is encrypted by the data identification information. The encrypted data identification information of the digital data and data control information, and the write identification information are encrypted by the use of recording medium identification information peculiar to the recording medium, and recorded to the recording medium along with the encrypted digital data.

The encrypted data identification information and data control information, and the write identification information recorded on the recording medium are read, and the encrypted data identification information and data control information are decrypted by the use of the write identification information.

According to the present invention, the independent write identification information is generated for each recording of the digital data, and the data identification information of the digital data and data control information are encrypted by the use of the generated write identification information, and at least the encrypted data identification information and data control information, and the write identification information are recorded to the recording medium. So, encrypting by the use of the recording medium identification information peculiar to the recording medium is performed for each recording of the digital data. Thus,

the data identification information cannot be decrypted even though the reproduced data from the recording medium is copied, which can prevent copying data.

The digital data is encrypted by the data identification information. Accordingly, the encrypted contents data cannot be decrypted as long as the data identification information cannot be decrypted.

When the data processing unit for encrypting the digital data and data recording unit for recording data to the recording medium are mounted separately, the data identification information cannot be decrypted even though the data transmitted between the data processing unit and data recording unit is monitored, which can prevent copying data.

These objects and other objects, features and advantages of the present intention will become more apparent from the following detailed description of the preferred embodiments of the present invention when taken in conjunction with the accompanying drawings.

## BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows a block diagram of a disc recording and/or reproducing apparatus and data processing apparatus employing the present invention.

Fig. 2 shows a block diagram for explaining the case in which the encrypted data is recorded by a disc recording and/or reproducing apparatus and reproduced by another disc recording and/or reproducing apparatus.

Fig. 3 shows a block diagram for explaining the case in which encrypted data recorded on a disc is copied to another disc and the copied encrypted data is reproduced.

Fig. 4 shows a block diagram for explaining the case in which the write identification information is transmitted without being encrypted.

Fig. 5 shows a block diagram for explaining the case in which the write identification information is encrypted and transmitted from the disc recording and/or reproducing apparatus to the data processing apparatus, and the encrypted data identification information and data control information are encrypted and transmitted from the data processing apparatus to the disc recording and/or reproducing apparatus.

## DESCRIPTION OF THE PREFERRED EMBODIMENTS

The data recording method and apparatus, data reproducing method and apparatus, and data recording and/or reproducing system according to the present invention will further be described below with reference to the accompanying drawings.

Fig. 1 shows a disc recording and/or reproducing apparatus 10 as a data recording apparatus according to the present invention, and a data processing apparatus 100 which may be a personal computer connected thereto.

The disc recording and/or reproducing apparatus 10 includes a spindle motor

11 to rotate a disc 30 being a removable disc-shaped recording medium such as a write-once type optical disc, rewritable type magneto-optical disc, or phase-change type optical disc, an optical pickup 12 to radiate a laser beam to the disc 30 and receive the returning laser beam, a laser driver 13 to drive a laser light source, not shown, such as a laser diode of the optical pickup 12, a signal detector 14 to detect an output signal from the optical pickup 12, a modulator/demodulator 15 to modulate a signal to the laser driver 13 and demodulate a signal sent from the signal detector 14, a buffer memory 16 to temporarily store data, an arbitrator 17, an ECC (Error Correction Code) unit 18 to perform error correction encoding/decoding, an I/F (interface) 19 to transmit/receive data to/from the data processing apparatus 100 such as a personal computer, and a write ID generator 20 to generate write ID (identification information) for each recording of data. The arbitrator 17 arbitrates data transmitted between the buffer memory 16, and modulator/demodulator 15, ECC unit 18 and I/F 19. The write ID from the write ID generator 20 is sent to the ECC unit 18, and is also sent to the external data processing apparatus 100.

The spindle motor 11 rotates the disc 30 at a constant linear velocity or constant angular velocity under the control of a servo circuit, not shown.

When recording data to the disc 30, a laser light source of the optical pickup 12 driven by the laser driver 13 radiates a laser beam to the disc 30 via an optical system such as an objective lens. When reproducing data recorded on the disc 30,

the laser light source of the optical pickup 12 radiates a laser beam to the disc 30 via the optical system, and a light-sensitive detector of the optical pickup 12 such as a photodiode receives the returning laser beam reflected and diffracted by the surface of the disc 30, and converts the received laser beam to an electric signal, and outputs the electric signal.

When recording/reproducing data to/from the disc 30, the optical pickup 12 performs tracking servo control and focusing servo control based on the detected signal of the returning laser beam.

The write ID generator 20 generates the write ID (identification information) being identification information peculiar to each recording (contents). This write ID is updated every time the data file is recorded, and is independent identification information for each recording operation. The write ID generated for each recording is different from each other, even though the recording operation is performed in the same disc apparatus and to the same disc. The write ID may be generated based on random numbers generated by, for example, a random number generator.

The disc recording and/or reproducing apparatus 10 further includes an encryptor/authenticator 21. The write ID generated by the write ID generator 20 may be transmitted to the data processing apparatus 100 without being processed, or may be encrypted by the encryptor/authenticator 21 and transmitted to the data processing apparatus 100, if necessary. When the write ID is encrypted and

transmitted to the data processing apparatus 100, the encryptor/authenticator 21 performs j ( ) encryption processing for the write ID, and transmits the encrypted write ID to the data processing apparatus 100 via the I/F 19. The encryptor/authenticator 21 also performs mutual authentication with the data processing apparatus 100.

The disc recording and/or reproducing apparatus 10 further includes a disc ID generator 23 and an encryptor 24. The disc ID generator 23 generates disc ID (disc identification information), which will be described later, and sends the disc ID to the encryptor 24 connected to the ECC unit 18. The write ID (write identification information) from the write ID generator 20 is also sent to the encryptor 24.

The encryptor 24 performs e ( ) encryption processing and f ( ) encryption processing for data to be recorded and the write ID, respectively, by the use of a key based on the disc ID, and sends the encrypted data to the ECC unit 18 via the arbitrator 17 and buffer memory 16. The encryptor 24 also performs $e^{-1}$ ( ) decryption processing and $f^{-1}$ ( ) decryption processing for data obtained from the ECC unit 18 via the arbitrator 17 and buffer memory 16 by the use of the key based on the disc ID.

The data processing apparatus 100, such as a personal computer, which is connected to the disc recording and/or reproducing apparatus 10, includes an I/F (interface) 101 to transmit/receive data to/from the disc recording and/or

reproducing apparatus 10, encryptor 102 to encrypt/decrypt data, a data processor 103 to process data in various manners, an authenticator 104 to perform mutual authentication with an external authentication institution etc., an I/F (interface) 105 to transmit/receive data identification information (contents ID, which will be described later) and data control information (for example, control information to restrict or prohibit copy generation) to/from an external unit, and an encryptor/authenticator 22 to decrypt the encrypted write ID from the I/F 101 and sends the decrypted write ID to the encryptor 102. The encryptor/authenticator 22 also performs mutual authentication with the disc recording and/or reproducing apparatus 10. The data processing apparatus 100 further includes an I/F (interface) 106 to receive encrypted contents data from outside, and a decryptor 107 to decrypt the encrypted contents data from the I/F 106 by the use of contents ID (data identification information). When the authentication is normally performed by the authenticator 104 and the user is proved to be authorized, the contents ID is sent from the data processor 103 to the decryptor 107.

Referring to Fig.2, the operation of the disc recording and/or reproducing apparatus 10 and data processing apparatus 100 configured as shown in Fig. 1 will be explained. The data processing apparatus 100, such as a personal computer, connected to the disc recording and/or reproducing apparatus 10 is configured such that encrypted contents ID and control information from the authentication institution or a key distribution center are supplied thereto via the I/F 105, and

encrypted contents data from a contents distribution center or contents provider is supplied thereto via the I/F 106. When the contents data is "u", contents ID to be used as a key to encrypt data is "cID", and encrypting is "c ( )", the encrypted contents data is represented as "c (u, cID)". When the control information is "cIN", and encrypting of the contents ID "cID" and control information "cIN" is "s ( )", the encrypted contents ID and control information are represented as "s (cID + cIN)".

Fig. 2 shows the case in which data recorded on a disc 30_0 obtained by recording data from the data processing apparatus 100_0 thereto by the disc recording and/or reproducing apparatus 10_0 is reproduced by another disc recording and/or reproducing apparatus 10_1. The encrypted contents data c (u_0, cID_0) and encrypted contents ID and control information s (cID_0 + cIN_0) are supplied to the data processing apparatus 100_0.

The data processing apparatus 100 performs mutual authentication with an authentication institution. When the data processing apparatus 100 is proved to be authorized, the encrypted contents ID and control information s (cID + cIN) are transmitted thereto. The authorized data processing apparatus 100 can decrypt the s (cID + cIN) and obtain contents ID cID to be used as a key for the encrypted contents data.

That is, in the example shown in Fig. 2, original contents ID and control information cID_0 + cIN_0 before encrypting can be obtained by performing $s^{-1}$ ( )

decryption processing for the encrypted contents ID and control information s (cID_0 + cIN_0) supplied to the data processing apparatus 100_0. The distributed encrypted contents data c (u_0, cID_0) is controlled by the control information cIN_0. In case the frequency of copying contents data is restricted, the control information cIN_0 is converted to cIN_1 by the data processor 103 when recording the contents data. The frequency of copying contents data is restricted or copying contents data is prohibited in accordance with the control information. Original contents data u_0 before encrypting can be obtained by decrypting the encrypted contents data c (u_0, cID_0) by the use of the decrypted contents ID cID_0.

The disc recording and/or reproducing apparatus 10_1 of Fig. 2 generates updated write ID, for example wID_0, for each recording of data, and performs j ( ) encryption processing for the wID_0 and outputs the encrypted wID_0 to the data processing apparatus 100_0. The data processing apparatus 100 _0 of Fig. 2 encrypts the contents ID and converted control information cID_0 + cIN_1 by the use of the write ID wID_0 obtained by decrypting the encrypted write ID j (wID_0) from the disc recording and/or reproducing apparatus 10_1, and generates encrypted data v (cID_0 + cIN_1, wID_0), and transmits the encrypted data to the disc recording and/or reproducing apparatus 10_1. The encrypted contents data c (u_0, cID_0) is transmitted to the disc recording and/or reproducing apparatus 10_1 without being processed.

The disc recording and/or reproducing apparatus 10_1 generates encrypted

data f (wID_0, dID_0) by performing f ( ) encryption processing for the write ID wID_0 generated for this recording by the use of disc ID dID_0 from the disc ID generator 23 of Fig. 1, and generates encrypted data e (v ( ), dID_0) by performing e ( ) encryption processing for the encrypted contents ID and control information v (cID_0 + cIN_1, wID_0) by the use of the disc ID dID_0. The v ( ) is the abbreviation for the v (cID_0 + cIN_1, wID_0). When performing f ( ) encryption processing and e ( ) encryption processing, the disc ID dID_0 as well as block ID which is identification information for each block being a recording unit can be used, if necessary. These encrypted data f (wID_0, dID_0) and v (cID_0 + cIN_1, wID_0) are recorded to the disc 30_0, and the encrypted contents data c (u_0, cID_0) from the data processing apparatus 100_0 is recorded to the disc 30_0 without being processed. The disc ID dID_0 is recorded to a predetermined region (toc, data recording region, etc.) of the disc 30_0 at the time of initialization, shipment, or first recording.

Next, the case in which data of the disc 30_0 is reproduced by the disc recording and/or reproducing apparatus 10_1 other than the disc recording and/or reproducing apparatus 10_0 will be explained.

The disc recording and/or reproducing apparatus 10_1 reproduces the encrypted data e (v ( ), dID_0) and f (wID_0, dID_0), and the encrypted contents data c (u_0, cID_0) from the disc 30_0, and reproduces the disc ID dID_0 from the predetermined region of the disc 30_0. The disc recording and/or reproducing

apparatus 10_1 obtains the encrypted contents ID and control information v (cID_0 + cIN_1, wID_0), and the write ID wID_0 by decrypting the reproduced encrypted data e (v ( ), dID_0) and f (wID_0, dID_0) by the use of the disc ID dID_0. The disc recording and/or reproducing apparatus 10_1 transmits the encrypted contents data v (u_0, wID_0) to the data processing apparatus 100_1 via the I/F, and performs j ( ) encryption processing for the write ID wID_0 and transmits the encrypted write ID data j (wID_0) to the data processing apparatus 100_1. The encrypted contents data c (u_0, cID_0) is transmitted to the data processing apparatus 100_1 without being processed.

The data processing apparatus 100_1 performs $j^{-1}$ ( ) decryption processing for the encrypted write ID data j (wID_0) to obtain the write ID wID_0, and takes out the contents ID and control information cID_0 + cIN_1 by decrypting the v (cID_0 + cIN_1, wID_0) from the disc recording and/or reproducing apparatus 10_1 by the use of the obtained write ID wID_0. The contents data u_0 can be obtained by decrypting the encrypted contents data v (u_0, wID_0) by the use of the contents ID cID_0. At this time, the decrypting is restricted by the control information cIN_1, or the control information cIN_1 itself is processed to be changed. For example, when the copied contents data u_0 is copied to another disc again, the control information cIN_1 is changed to control information cIN_2.

According to the present invention configured as described above, the disc ID dID and write ID wID become unrelated to each other, which can prevent the

disc ID dID and write ID wID from being taken out to outside from the disc recording and/or reproducing apparatus 10 and data processing apparatus 100. The disc recording and/or reproducing apparatus 10 does not have to know the v ( ) encryption processing for the contents ID and control information. The data processing apparatus 100 performs the v ( ) encryption processing on its own responsibility. And, the disc recording and/or reproducing apparatus 10 performs the e ( ) encryption processing and f ( ) encryption processing on its own responsibility. Thus, the security of the interfaces between the disc recording and/or reproducing apparatus 10 and data processing apparatus 100, and that of recording/reproducing data to/from the disc 30 by the disc recording and/or reproducing apparatus 10 can be independent.

Fig. 3 shows the case in which disc copy is prevented by encrypting data by the use of the write ID.

In Fig. 3, the data processing apparatus 100_0, data processing apparatus 100_1, disc recording and/or reproducing apparatus 10_0, and disc recording and/or reproducing apparatus 10_1 are identical with those in Fig. 2. So, the elements or parts will be indicated with the same or similar reference numerals, and the explanation will be omitted. In Fig. 3, the encrypted contents ID and control information v (cID_0 + cIN_1, wID_0) and encrypted contents data v (u_0, cID_0) from the disc recording and/or reproducing apparatus 10_1 are transmitted to another disc recording and/or reproducing apparatus 10_2 and recorded to another

disc 30_2.

The disc recording and/or reproducing apparatus 10_1 obtains the encrypted data f (wID_0, dID_0) and e (v ( ), dID_0) by reproducing the data recorded on disc 30_0, and obtains the encrypted contents ID and control information v (cID_0 + cIN_1, wID_0), and the write ID wID_0 by decrypting the reproduced encrypted data f (wID_0, dID_0) and e (v ( ), dID_0) by the use of the disc ID dID_0 recorded to the predetermined position of the disc 30_0. The disc recording and/or reproducing apparatus 10_1 obtains the encrypted contents data c ( ), that is c (u_0, cID_0) by reproducing the data recorded on the disc 30_0. The encrypted data v (cID_0 + cIN_1, wID_0) and encrypted contents data c ( ) obtained from the disc recording and/or reproducing apparatus 10_1 are transmitted to the disc recording and/or reproducing apparatus 10_2 without being processed, and recorded to another disc 30_2. The disc recording and/or reproducing apparatus 10_2 generates disc ID dID_2 corresponding to the disc 30_2 and records the disc ID dID_2 to a predetermined position of the disc 30_2, and generates write ID wID_2 when recording data, and encrypts the write ID wID_2 and encrypted data v (cID_0 + cIN_1, wID_0) by the use of a key based on the disc ID dID_2, and records thus obtained encrypted data e (v ( ), dID_2) and f (wID_2, dID_2) to the disc 30_2.

When reproducing data recorded on the disc 30_2 by a disc recording and/or reproducing apparatus 10_3, the encrypted data e (v ( ), dID_2) and f (wID_2, dID_2) recorded on the disc recording and/or reproducing apparatus 10_2 are

reproduced and transmitted to a disc recording and/or reproducing apparatus 10_3. The encrypted contents data c ( ) is reproduced from the disc 30_2 and transmitted to the disc recording and/or reproducing apparatus 10_3. The disc recording and/or reproducing apparatus 10_3 reads the disc ID dID_2 recorded on a predetermined position of the disc 30_2, and decrypts the encrypted data e (v ( ), dID_2) and f (wID_2, dID_2) by the use of a key based on the disc ID dID_2. Thus, the copied encrypted data v (cID_0 + cIN_1, wID_0) and write ID wID_2 generated when recording the encrypted data v (cID_0 + cIN_1, wID_0) to the disc 30_2 are restored. The encrypted data v (cID_0 + cIN_1, wID_0) are transmitted to the data processing apparatus 100_3 without being processed. The disc recording and/or reproducing apparatus 10_3 performs $j^{-1}$ ( ) decryption processing for the write ID wID_2, and the encrypted write ID wID_2 is transmitted to the data processing apparatus 100_3. The data processing apparatus 100_3 performs $j^{-1}$ ( ) decryption processing for the encrypted write ID j (wID_2) to obtain the write ID wID_2, and tries to decrypt the encrypted data v (cID_0 + cIN_1, wID_0) from the disc recording and/or reproducing apparatus 10_3 by the use of the write ID wID_2. However, since the encrypted data v (cID_0 + cIN_1, wID_0) are encrypted by the use of a key based on the write ID wID_0, the encrypted data v (cID_0 + cIN_1, wID_0) can not be decrypted. Thus, original data, that is contents ID and control information cID_0 + cIN_1 can not be obtained.

That is, the data processing apparatus 100_3 receives the write ID wID_2.

On the other hand, the encrypted data v (cID_0 + cIN_1, wID_0) are encrypted by the write ID wID_0. Thus, it can be seen that illegal copy is performed from this disaccord of the write ID. Since the encrypted data v (cID_0 + cIN_1, wID_0) can not be decrypted by the write ID wID_2, original contents ID and control information cID_0 + cIN_1 can not be obtained.

It can be considered that, when performing disc copy, reproduced data from the disc recording and/or reproducing apparatus 10_1 is recorded by means of the disc recording and/or reproducing apparatus 10_0 which records original data. However, since updated write ID is generated , and the write ID is different from the write ID wID_0 generated at the time of recording original data. Thus, decrypting can not be performed either.

Fig. 4 shows the case in which the write ID is transmitted from the disc recording and/or reproducing apparatus 10 to the data processing apparatus 100 without being encrypted. Other than this, the elements or parts will be indicated with the same or similar reference numerals in Fig. 2. So, the explanation will be omitted.

Fig. 5 shows the case in which the write ID as well as the encrypted contents ID and control information v (cID_0 + cIN_1, wID_0) is encrypted and transmitted between the disc recording and/or reproducing apparatus 10 and data processing apparatus 100.

That is, when recording data, encrypted data j (wID_0) obtained by

performing j ( ) encryption processing for the write ID wID_0 generated by the disc recording and/or reproducing apparatus 10_1 is transmitted to the data processing apparatus 100_0. The data processing apparatus 100_0 encrypts the contents ID and control information cID_0 + cIN_1 by the use of the write ID wID_0 obtained by decrypting the encrypted data j (wID_0) to generate the encrypted data v (cID_0 + cIN_1, wID_0), and performs j ( ) encryption processing for the encrypted data v (cID_0 + cIN_1, wID_0), and transmits the encrypted data to the disc recording and/or reproducing apparatus 10_1.

When reproducing data, the disc recording and/or reproducing apparatus 10_1 decrypts the encrypted data e (v ( ), dID_0) and f (wID_0, dID_0) obtained by reproducing data recorded on the disc 30_0 by the use of the disc ID dID_0 reproduced from the disc 30_0 to obtain the write ID wID_0 and encrypted data v (cID_0 + cIN_1, wID_0), and performs j ( ) encryption processing for the write ID wID_0 and encrypted data v (cID_0 + cIN_1, wID_0), and transmits thus obtained encrypted data j (wID_0) and j (v ( )) to the data processing apparatus 100_0. The data processing apparatus 100_0 performs $j^{-1}$ ( ) decryption processing for the encrypted data j (wID_0) and j (v ( )) to obtain the wID_0 and v (cID_0 + cIN_1, wID_0).

In Fig. 5, the elements or parts will be indicated with the same or similar reference numerals in Fig. 2, and the explanation is omitted.

The present invention is not restricted to the above-mentioned embodiments.

In the embodiments, the data processing unit and disc recording and/or reproducing unit are mounted in independent apparatuses. On the other hand, the data processing unit and disc recording and/or reproducing unit can be mounted in independent substrates mounted in the same apparatus, or in independent circuits mounted in the same substrate. The recording medium is not restricted to the disc-shaped recording medium, and my be a card-shaped or tape-shaped recording medium. The user data can be data which is not encrypted, or data which has already been encrypted by another encrypting key. Furthermore, the write ID as well as recording medium ID (disc ID etc.) peculiar to a recording medium such as a disc, and block ID peculiar to a block (sector, frame, etc.) being a unit for encoding or a unit for recording. In this case, random number generators for generating the write ID, disc ID, and block ID can be common. Various modifications can be possible without departing from the spirit and scope of the present invention.